RAPID LABS

SMART CONTRACT SECURITY AUDIT

Final report **Plan: Simple**

Umbrella Protocol

August 2022

RL@RAPIDLABS.FINANCE RAPIDLABS.FINANCE

TABLE OF CONTENTS

INTRODUCTION

Implementation of ERC-20 token standard with fees on transfers. Fees are used to buy back reward token in uniswap pair.

Name	Umbrella Protocol
Audit date	2022-08-15 - 2022-08-17
Language	Solidity
Platform	Binance Smart Chain

ANALYZED CONTRACTS

Name	Address
DividendDistributor	0x2238fefbb7f27a53a5f870021a30815bd5023f6c
BuybackBabyToken	0x2238fefbb7f27a53a5f870021a30815bd5023f6c
Clones	0x2238fefbb7f27a53a5f870021a30815bd5023f6c

AUDIT PROCESS

Our audit structure consists of two stages:

Auto-analysis

- Our automated tools allow us to scan smart contract code and find potential issues
- We hand pick and verify all the issues found by the tools

Expert audit

- Manual analysis of potential issues and vulnerabilities

- Contract code is reviewed thoroughly

KNOWN ISSUES CHECKED

Title	Result
Unencrypted Private Data On-Chain	✓ passed
Code With No Effects	✓ passed
Message call with hardcoded gas amount	✓ passed
Typographical Error	✓ passed
DoS With Block Gas Limit	✓ passed
Presence of unused variables	✓ passed
Incorrect Inheritance Order	✓ passed
Requirement Violation	✓ passed
Weak Sources of Randomness from Chain Attributes	✓ passed
Shadowing State Variables	✓ passed
Incorrect Constructor Name	✓ passed

Block values as a proxy for time	✓ passed
Authorization through tx.origin	✓ passed
DoS with Failed Call	✓ passed
Delegatecall to Untrusted Callee	✓ passed
Use of Deprecated Solidity Functions	✓ passed
Assert Violation	✓ passed
State Variable Default Visibility	✓ passed
Reentrancy	✓ passed
Unprotected SELFDESTRUCT Instruction	✓ passed
Unprotected Ether Withdrawal	✓ passed
Unchecked Call Return Value	✓ passed
Floating Pragma	✓ passed
Outdated Compiler Version	✓ passed
Integer Overflow and Underflow	✓ passed
Function Default Visibility	✓ passed

ISSUE CLASSIFICATION

High risk	Issues leading to assets theft, locking or any other loss of assets or leading to contract malfunctioning.
Medium risk	Issues that can trigger a contract failure of malfunctioning.
Low risk	Issues that do now affect contract functionality. For example, unoptimised gas usage, outdated or unused code, code style violations, etc.

ISSUES

High risk issues

1. No error handling (BuybackBabyToken)

_transferFrom() and swapBack() functions contain empty try/catch blocks in case of reward token transfer failure. Therefore, users' shares may become unfair and inconsistent.

2. Excessive owner's rights (BuybackBabyToken)

    1. The owner can exclude any address from dividends reception;
    2. The owner can update the swapThreshold variable with a wrong value. This may halt the distribution of the fees for a long period of time. Enabling back swaps and liquidity adding may lead to the token price wrecking if the contract's balance is comparable to a pair reserves.

Medium risk issues

1. Swaps with 100% slippage (BuybackBabyToken)

swapExactTokensForETHSupportingFeeOnTransferTokens() and swapExactETHForTokensSupportingFeeOnTransferTokens() functions call router with 100% slippage. The transactions sent from this contract may be front-runned resulting in swaps with an

undesired rate (sandwich attacks).

Low risk issues

1. Gas optimisation (DividendDistributor)
    1. rewardToken, router, _token should be marked immutable;
    2. dividendsPerShareAccuracyFactor shoud be const;

2. Lack of events (DividendDistributor)

No events are emittied in setShare(), deposit(), distributeDividend(), setDistributionCriteria()

3. Redundant code (BuybackBabyToken)

Setter function and access modifactor for buyBackers are not applyied anywhere.

4. Lack of events (BuybackBabyToken)

No events are emitted in setFeeReceivers(), setSwapBackSettings(), setTargetLiquidity(), setDistributorSettings(), setFees(), setIsFeeExempt().

5. Gas optimization (BuybackBabyToken)

_name, _symbol, _totalSupply, router, pair should be marked as immutable.

6. Redundunt code (Clones)

The library is not used in the contract.

CONCLUSION

Umbrella Protocol DividendDistributor, BuybackBabyToken, Clones contracts were audited. 2 high, 1 medium, 6 low risk issues were found.

DISCLAIMER

This report is subject to the terms and conditions (including without limitation, description of services, confidentiality, disclaimer and limitation of liability) set forth in the Services Agreement, or the scope of services, and terms and conditions provided to the Company in connection with the Agreement. This report provided in connection with the Services set forth in the Agreement shall be used by the Company only to the extent permitted under the terms and conditions set forth in the Agreement. This report may not be transmitted, disclosed, referred to or relied upon by any person for any purposes without RapidLabs prior written consent.

This report is not, nor should be considered, an "endorsement" or "disapproval" of any particular project or team. This report is not, nor should be considered, an indication of the economics or value of any "product" or "asset" created by any team or project that contracts RapidLabs to perform a security assessment. This report does not provide any warranty or guarantee regarding the absolute bug-free nature of the technology analyzed, nor do they provide any indication of the technologies proprietors, business, business model or legal compliance.

This report should not be used in any way to make decisions around investment or involvement with any particular project. This report in no way provides investment advice, nor should be leveraged as investment advice of any sort. This report represents an extensive assessing process intending to help our customers increase the quality of their code while reducing the high level of risk presented by cryptographic tokens and blockchain technology.

RAPID LABS

YOUR PROJECT SECURED

RL@RAPIDLABS.FINANCE

RAPIDLABS.FINANCE